PAT.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,164	01/14/2000	Daniel Jay Thomsen	105.174US1	8029

7590 09/15/2003

Schwegman Lundberg Woessner & Kluth PA
P O Box 2938
Minneapolis, MN 55418

EXAMINER
SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
2134	6

DATE MAILED: 09/15/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PRE

Office Action Summary	Application No.	Applicant(s)	
	09/483,164	THOMSEN ET AL.	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19, 21-28 and 30-38* is/are rejected.

7)☒ Claim(s) *15, 17, 20 and 29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-38 are pending.

2. The IDS of 9/19/2001 has been received and considered.

Specification

3. The disclosure is objected to because of the following informalities:

On page 6, line 12, "System 10 uses an layered" should use "a" instead of "an".

On page 24, line 14, "net work" should be one word.

On page 25, line 12, "per form" should be one word.

On page 28, line 30, "ex amine" should be one word.

On page 29, line 20, the "¡" character should be replaced with "-".

On page 32, line 10, "a method for adding an removing" should use "and" instead of "an".

Appropriate correction is required.

4. The disclosure is objected to because of the following informalities:

On page 18, line 14, reference to "Figs. 11a and b" should be replaced with "Figs. 13a and b".

Appropriate correction is required.

Claim Objections

5. Claims 15, 17, 20 and 29 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The claims state "wherein combining one or more keys to form a key chain includes", but "combining one or more keys to form a key chain" in both independent claims 14 and 22 is made in reference to the application policy layer, the first semantic policy layer, the second semantic policy layer and the local policy layer. Therefore, claims 15, 17, 20 and 29 fail to further limit the subject matter of the claims 14 and 22.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

7. Claims 1-35 are rejected under 35 U.S.C. 102(a) as being anticipated by printed publication "Role Based Access Control Framework for Network Enterprises" by Thomsen, O'Brien and Bogle. The publication describes a system in which application-specific security mechanisms are encapsulated into keys. The keys can be linked, forming chains, which can be again encapsulated to form keys (see §2.4, §2.6 and figure 2). The keys can be passed to other

layers (see §4). The publication describes associating key chains with users (see figure 4) and translating and exporting a security policy where a policy is enforced (see §3.1).

8. Claims 1-3, 5-8, 14-16, 22-24, 30, and 32-34 are rejected under 35 U.S.C. 102(b) as being anticipated by "Issues in the Design of Secure Authorization Service for Distributed Applications" by Crall et al. (Crall), published November 1998.

Regarding claims 1, 3, 5-7, 14, 22, 30, 32 and 34, Crall discloses a security framework for addressing the needs of "several classes of users" comprising a graphical user interface (see page 874, §1). The system pushes authorization information to a specific target (see page 876, §2.2) to enforce access to resources. Crall further discloses a system with three levels of abstraction concerned with authorization management (see page 874, §2). Privileges represent authorization to access application-specific resources, entitlements (encapsulated privileges) represent authority to perform tasks and profiles represent groups or classes allowed the same entitlements or privileges (see pages 879-879, §4). Entitlements can then be combined through Boolean expressions (see page 8787, §4), and assigned to profiles to form another abstracted level of authorizations. Users and groups of users are assigned to profiles, the policy is pushed to the target(s) and the target enforces the security policy (see page 876, §2.2).

Regarding claim 2, Crall discloses administration and management of security policies in a distributed computing environment (see page 874, ABSTRACT and §1).

Regarding claim 8, Crall discloses using profiles to assign privileges to users who perform the roles (see page 875, §2.2 and 879, §4).

Regarding claims 15, 16 and 23, Crall discloses entitlements having one or more privileges or one or more sets of privileges (see page 878, §4).

Regarding claim 24, Crall discloses assigning users to profiles, which can contain entitlements and privileges (see page 879, §4).

Regarding claims 21 and 30, Crall discloses assigning local users to one or more policies (see page 879, §4).

9. Claims 36-38 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 6,088,679 to Barkley. Barkley discloses a workflow management system employing a RBAC (role-based access control) system wherein according to defined roles, groups or users are associated with, by the RBAC system, the permissions, tools and resources necessary to complete a particular step of the workflow (see col. 5, lines 49-54 and 56-67 and col. 6, lines 1-5). Any needed applications are invoked and roles are then activated at appropriate points in the process, thereby giving permissions to access resources (see col. 6, lines 6-12).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 4, 9, 10, 11-13, 17, 25-26 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crall in view of "The ARBAC97 Model for Role-Based Administration of Roles" by Sandhu et al. (Sandhu).

Regarding claims 4 and 10, Crall discloses an authorization system as described above, but lack a means for drilling to a lower layer to customize security policies. Sandhu discloses a "UP-Roles" structure, which can contain both abstracted abilities and permissions themselves. An administrator, therefore, can assign a UP-role, which can include existing "abilities" or policies and then add additional permissions (see page 122, §5) to maximize flexibility and enforce *least privilege* (see page 106, 3rd paragraph). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Crall to allow administrators to use less-abstracted permissions, from lower layers, with profiles to gain the benefit of granting users only roles that must be invoked to complete a task, as taught by Sandhu.

Regarding claim 9, Crall discloses a multi-level security system as described above, but lack disclosure of grouping the layers in a partially ordered set. Sandhu teaches that organizing roles in a partial order so the roles can benefit from inheritance, making indirect role assignment possible (see page 107, §2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Crall to group roles in a partially ordered set, so as to gain the benefit of inheritance, as taught by Sandhu.

Regarding claims 11, 17, 25 and 26, Crall discloses a multi-level security system for different classes of users as described above, but the system lacks constraints. Sandhu et al. teach that constraints are a "powerful mechanism for laying out higher-level organizational

policy", useful in enforcing the principle of separation of duties (see page 108, 1st paragraph). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Crall by attaching one or more constraints to a role to enforce separation of duties, as taught by Sandhu.

Regarding claims 12 and 13, Crall discloses a system with three levels of abstraction concerned with authorization management of several classes of users (see page 874, §2). Privileges represent authorization to access application-specific resources, entitlements represent authority to perform tasks and profiles represent groups or classes allowed the same entitlements or privileges (see pages 879-879, §4). Key attributes, which are subsets of privileges, are assigned to various entitlements, creating an abstracted level of authorizations. Entitlements can then be combined through Boolean expressions (see page 8787, §4), and assigned to profiles to form another abstracted level of authorizations. Users and groups of users are assigned to profiles, and the target enforces the security policy (see page 876, §2.2).

Regarding claims 18, 19, 27 and 28, Crall discloses a system as modified described above, but lacks grouping application methods as handles. Sandhu teaches that, in the role-based model, application developers packaging permissions to access computer resources into collections, labeled 'abilities', so a single unit could be designated for a role (see page 122, §5). Sandhu further teaches that abilities can include other abilities (see page 122, §5), allowing division as necessary on a per-application basis. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Crall to specifically group application methods as permissions and to assign one or more permissions to users, allowing roles to be designated encapsulated, application-specific access.

12. Claims 31 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crall et al. in view of "The ARBAC97 Model for Role-Based Administration of Roles" by Sandhu et al. (Sandhu) in further view of "Access Control: Principles and Practice" by Samarati et al. (Samarati), published September 1994. Crall discloses a security system as modified above, and further discloses a graphical user interface (see page 874, §1) used by administrators to manage a large group of users; such functions include removing privileges (see page 878, §3.2). Crall's system lacks a partial-order organization. Sandhu teaches that organizing roles in a partial order is beneficial because the roles can inherit attributes from other roles, making indirect role assignment possible (see page 107, §2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Crall's system to group roles in a partially ordered set, so as to gain the benefit of inheritance, as taught by Sandhu. The system of Crall, as modified above, lacks a role hierarchy graph. Samarati teaches that in many applications, a hierarchy of roles exists, and that hierarchical roles "further simplify authorization management" (see page 46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Crall's system to display a role hierarchy graph to further simplify management for administrators.

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191.

The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:30 p.m.. The examiner can also be reached on alternate Fridays from 8:00 a.m. – 4:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

4 September 2003
MJS

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100